



COMDTINST 5230.67
AUG 30, 2004

COMMANDANT INSTRUCTION 5230.67

Subj: COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INFORMATION
TECHNOLOGY (C4&IT) INFORMATION ASSURANCE (IA) POLICY

Ref: (a) Establishment of the CG-6 Directorate and Associated Duties, COMDTINST 5401.5
(series)

1. PURPOSE. This Instruction establishes the authority, roles, and responsibilities governing the enterprise Information Assurance (IA) program. The IA program addresses information protection, detection, and reaction for Command, Control, Communications, Computers and Information Technology (C4&IT) systems, identifies system vulnerabilities, establishes disaster recovery procedures, and manages the IA security awareness and education program. A robust IA program defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This policy applies to C4&IT assets, including systems and products that enable C4&IT capability in support of the Coast Guard's missions or business functions. For systems governed by separate IA authorities, as listed in the C4&IT System Inventory, this policy governs the interfaces between those systems and other Coast Guard C4&IT systems. All Coast Guard organizations involved in the planning, acquisition, production, deployment, support, operation, and disposition of C4&IT assets shall employ the IA policy and adhere to the roles defined herein.
2. ACTION. Area and District commanders, commanders of maintenance and logistics commands, commanding officers of Headquarters units, assistant commandants for directorates, Chief Counsel, and special staff offices at Headquarters shall ensure that all Coast Guard and contractor support personnel or organizations involved in the acquisition, development, operations, maintenance, or use of Coast Guard C4&IT assets comply with the provisions of this Instruction. Internet release is authorized.
3. DIRECTIVES AFFECTED. None

DISTRIBUTION – SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1	1	1	1																				
B		8	10		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1				2	1	1	2			1								1	
D	1	1		1	1															1						
E															1								1			
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION:

4. **INFORMATION ASSURANCE ROLES AND RESPONSIBILITIES.** The Commandant (CG-6) organization works proactively with all entities involved in the system life cycle. Figure 1: CG-6 Roles and Relationships Framework, illustrates the key roles involved and their relationships. The remainder of this paragraph describes the roles, relationships, and responsibilities as they relate to this policy.

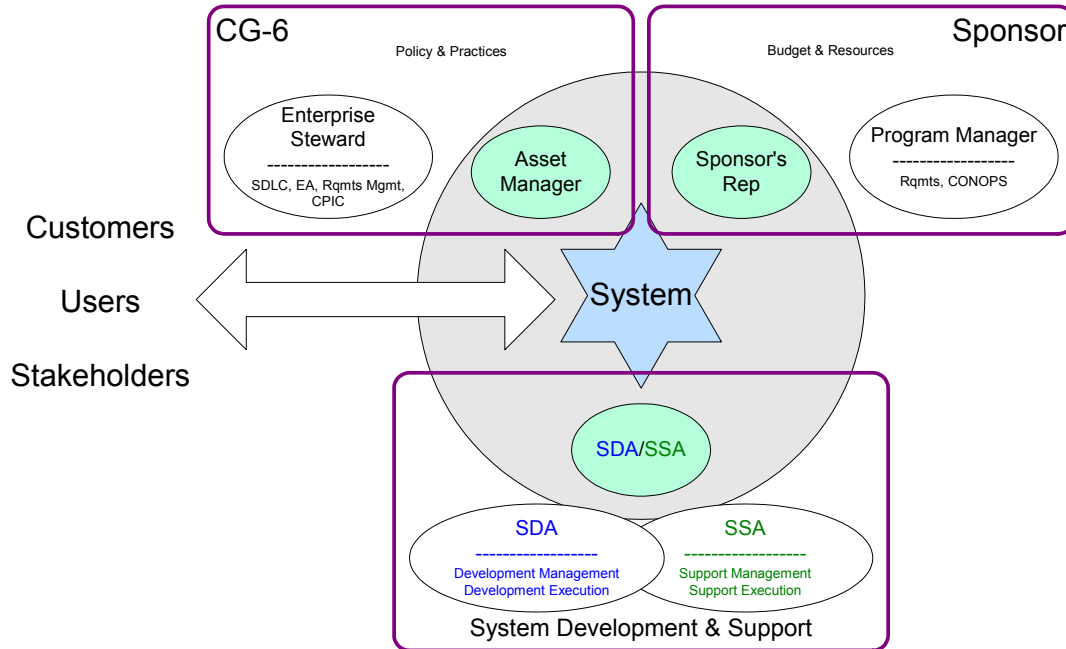


Figure 1: CG-6 Roles and Relationships Framework

- a. **CG-6.** The Chief Information Officer (CIO). The CIO is responsible for implementing IA throughout the Coast Guard. The CIO shall lead the IA program by partnering with all Sponsors and Program Managers to plan, design, develop, deploy, and maintain C4&IT systems that incorporate robust IA safeguards designed to meet Coast Guard-wide mission and business requirements and minimize risk to Coast Guard C4&IT systems, information, and personnel. CG-6 has the following IA responsibilities:
- (1) Maintaining and approving IA policy and practices. CG-6 shall establish an IA Policy Review Board, comprising representatives from various stakeholder groups, to develop and maintain IA policy and practices.
 - (2) Ensuring that the IA program is developed and managed in accordance with Federal IT laws and policy, national and international standards, Department of Homeland Security (DHS) policies and standards, applicable Department of Defense (DoD) policy and standards, and specific Memoranda of Understanding between the Coast Guard and other agencies.
 - (3) Ensuring that IA is an integral part of life cycle management for all C4&IT systems developed or maintained within the Coast Guard.
 - (4) Designating Coast Guard organizations or individuals to develop and maintain the practices and products that support and implement IA. These designations shall be published and kept current by CG-6.
 - (5) Delegating authority to the Delegated Accrediting Authority (DAA) to issue or withdraw the authority to operate or connect.

- (6) Delegating the execution of IA practices to the roles defined herein.
- b. Enterprise Steward. CG-6 provides enterprise-level stewardship of the policies and practices associated with C4&IT systems. The Enterprise Steward monitors the health, effectiveness, and efficiency of IA and ensures organizational compliance. The Enterprise Steward has the following IA responsibilities:
 - (1) Managing the IA process. This includes developing and sustaining practices for Certification and Accreditation, Security Management, and IA Architecture.
 - (2) Proactively communicating, educating, and training Coast Guard C4&IT personnel in IA practices to ensure effective implementation of IA in all stages of the life cycle.
 - c. Asset Manager. The Asset Manager is designated by CG-6 to guide, oversee, and monitor IA policies and practices for an assigned system. An asset is a system, product (e.g., Commercial-off-the-Shelf equipment, information, policy), data, service, capability, or resource that is available, managed, delivered, applied, supported, or sustained on an enterprise scale by the CG-6 organization in collaboration with its supporting program sponsor and manager, customers, and external stakeholders, System Development Agent (SDA), and System Support Agent (SSA). The Asset Manager shall collaborate with the Sponsor's Representative, SDA, and SSA to ensure alignment and compliance with the Coast Guard's System Development Life Cycle (SDLC) policies and practices. The Asset Manager has the following IA responsibilities:
 - (1) Ensuring that resource estimates are realistic and adequate and have considered IA in all aspects of the SDLC.
 - (2) Collaborating with the Sponsor's Representative, SDA, and SSA to facilitate alignment and compliance with Coast Guard IA policies and practices.
 - (3) Maintaining a set of metrics to ensure that IA is being met during system development, performance, and maintenance.
 - (4) Developing and recommending changes to IA policies and practices, as necessary, to enhance the quality of C4&IT IA practices.
 - (5) Facilitating resolution of issues among the Sponsor's Representative, SDA, SSA, and other programs.
 - d. Sponsor. The Sponsor is the organizational element that articulates goals, validates requirements, acquires resources, and accepts C4&IT capability needed to support a Coast Guard mission. The Sponsor has the following IA responsibilities:
 - (1) Ensuring that IA requirements are addressed throughout the life cycle of each system.
 - (2) Ensuring that resources are available for IA practices, that these practices are followed, and that the system can operate at an acceptable level of risk prior to receiving Authority to Operate the system.
 - (3) Coordinating with the network DAA to receive Authority to Connect.
 - (4) Designating the Sponsor's Representative.
 - (5) Designating the Program Manager.
 - e. Program Manager. The Program Manager is the Sponsor's designated manager who is responsible for development and production of program requirements. The Program Manager advocates the end user's concerns and establishes or maintains mechanisms to ensure that the

user's needs are being addressed throughout the life cycle. The Program Manager has the following IA responsibilities:

- (1) Incorporating IA initiatives pertinent to each C4&IT system and managing the Plan of Action and milestones to mitigate known risks.
 - (2) Collecting and coordinating input from end users, enterprise application owners, operations and maintenance communities, and other stakeholders, and using this input to develop functional requirements.
 - (3) Developing performance measures that quantify the IA program's success in mitigating risks to C4&IT across the enterprise and balancing risks against response time and information accessibility and connectivity. The Program Manager provides these measures to the Asset Manager.
 - (4) Developing and promulgating the Concept of Operations for each C4&IT system.
 - (5) Developing acceptance criteria for each C4&IT system.
- f. Sponsor's Representative. The Sponsor's Representative is designated by the Sponsor to serve as the liaison and interface for the Sponsor and the Program Manager to the other key roles involved in C4&IT management. The Sponsor's Representative has the following IA responsibilities:
- (1) Validating functional requirements and ensuring that IA is considered and integrated throughout the life cycle.
 - (2) Maintaining liaison with the Asset Manager, the Sponsor, and technical staffs of the SDA and SSA.
 - (3) Representing all of the Sponsor's needs.
 - (4) Developing cost estimates in collaboration with the CG-6 Asset Manager, who will collect and assimilate appropriate SDA and SSA input.
 - (5) Allocating resources necessary to implement IA. The Sponsor's Representative prepares the business case and other justification for the Sponsor to use in acquisition of resources.
- g. System Development Agent (SDA). The SDA is the individual, unit, firm, agency, or organization that performs, or has the responsibility for, the design, development, implementation, and support of the C4&IT system, as well as the acquisition of C4&IT products or services. The SDA has a critical role in IA. The SDA either implements all IA practices for assigned systems or is a technical advisor to the other stakeholders involved in IA. More than one SDA may be involved in the various aspects of IA. The SDA has the following IA responsibilities:
- (1) Carrying out approved IA practices for assigned systems.
 - (2) Coordinating IA system activities from the conceptual planning phase through the implementation phase.
 - (3) Developing a set of measurements to determine the degree of compliance to IA standards for a developing system. The SDA provides these measures to the Asset Manager.
 - (4) Providing competent technical authority for IA practices in the current version and for IA changes under consideration.

- (5) Collaborating with the Sponsor's Representative, SSA, and the Asset Manager to refine employed IA practices.
- (6) Developing and submitting technical proposals to implement IA changes, as appropriate.
- h. System Support Agent (SSA). The SSA is the individual, unit, firm, agency, or organization that performs, or has responsibility for, the maintenance, support, and availability of C4&IT systems. The SSA participates in all aspects of IA. The SSA has the following IA responsibilities:
 - (1) Coordinating IA system activities from the implementation phase through the remainder of the life cycle.
 - (2) Supporting the SDA and other IA stakeholders as a technical advisor for IA issues, from the field perspective, throughout the life cycle.
 - (3) Developing a set of metrics to determine the continued validity of IA for a given system or service. The SSA provides these measurements to the Asset Manager.
 - (4) Providing competent technical authority for identifying, developing, and resolving support requirements associated with IA changes.
 - (5) Collaborating with the Sponsor's Representative, SDA, and the Asset Manager to define support requirements and support solutions.
- i. User. The user is the individual, unit, or organization that interacts with and uses C4&IT systems or services to accomplish work, execute missions, or deliver products and services to Coast Guard members and external customers. The user provides feedback on existing C4&IT systems, suggests enhancements to existing C4&IT systems, or identifies new system requirements via the Sponsor's Representative.
- j. Customer. A customer is any person or organization that benefits from C4&IT systems or services. An internal customer is a person or organization inside the Coast Guard for which the C4&IT system or service is being provided. An external customer is a person or organization outside the Coast Guard for which the C4&IT product or service is being provided. The customer provides feedback on existing C4&IT systems, suggests enhancements to existing C4&IT systems, or identifies new system requirements via the Sponsor's Representative.
- k. Stakeholder. For IA, a stakeholder is any person, group, or organization (e.g., customers; employees; suppliers; owners; Office of Management and Budget, DHS, or other agencies; and Congress) that can place a claim on, or influence, a C4&IT asset, is affected by that asset, or has a vested interest in or expectation for the asset. The stakeholder provides feedback on existing C4&IT systems, suggests enhancements to existing C4&IT systems, or identifies new system requirements via the Sponsor's Representative.
- l. Designated Accrediting Authority (DAA). The DAA is a senior management official responsible for approving the operation of a C4&IT system at an acceptable level of risk. The DAA issues (or withdraws) the Authority to Operate a system. The DAA may issue an Interim Authority to Operate when a mitigation strategy has been developed and funded and risk exists. The DAA shall be an Assistant Commandant, Area, or Maintenance and Logistics Command (MLC) Flag Officer or Senior Executive Service employee. The duties of the DAA may be delegated to an O-6, GS-15, or above and will not be delegated below this level without written approval from the CIO.
- m. Certifying Authority (CA). The CA shall be assigned to each C4&IT system or activity. The CA is responsible for documenting the IA posture (e.g., security plan, POA&M, DR Plan,

ST&E) of a system or activity. The CA submits the accreditation package to the DAA for approval. The CA is equivalent to the Certifying Official.

- n. Information System Security Program Officer (ISSPO). The ISSPO shall be assigned to each C4&IT system. The ISSPO is a government employee responsible to the DAA for ensuring the security of a system or activity throughout its life cycle. An ISSPO is a staff assignment at the Area, MLC, District, or Headquarters unit.
 - o. Information Systems Security Officer (ISSO). The ISSO develops and executes the system's security plan. The ISSO is either government or contractor personnel. Where an ISSO is assigned, the ISSO is responsible for assisting the ISSPO in performing the day-to-day duties of safeguarding information in support of the IA program and the cognizant ISSPO.
 - p. Alternate Information Systems Security Officer (AISSO). The AISSO is either government or contractor personnel with an appropriate security clearance. Where an ISSO is assigned, the AISSO assists the ISSO and also performs the day-to-day duties of safeguarding information in support of the ISSO.
 - q. Information System Security Manager (ISSM). The ISSM is the Coasts Guard's principal advisor on information security matters. The ISSM is responsible for development and maintenance of IA policies and practices.
5. IMPLEMENTATION. IA practices establish the actions necessary to implement the IA program. All Coast Guard organizations involved in the planning, acquisition, production, deployment, support, operation, and disposition of C4&IT systems shall follow IA practices. CG-6 charters and delegates the primary development, maintenance, and review responsibility for IA practices to the IA Policy Review Board. CG-6 has final approval authority for these practices. The IA practices provide the procedures and process for the following:
- a. Certification and Accreditation. Procedures to complete certification and accreditation of major applications and general support systems are described in National Institute of Standards and Technology Special Publication 800-series, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, Security Self-Assessment Guide for Information Technology Systems, and the Department of Defense, DoD 8510 series, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) or successor.
 - b. Security Management. Security Management describes various practices needed to manage information security throughout the life cycle of C4&IT systems.
 - c. Information Assurance Architecture. The IA Architecture is the framework that ensures the integration of Enterprise Architecture, the SDLC, and Configuration Management practices with IA policies and practices. This framework supports certification and accreditation activities and determination of risk acceptability.

6. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined to be not applicable.
7. FORMS/REPORTS. None

C.I. PEARSON /s/
Assistant Commandant for Command, Control,
Communications, Computers and
Information Technology